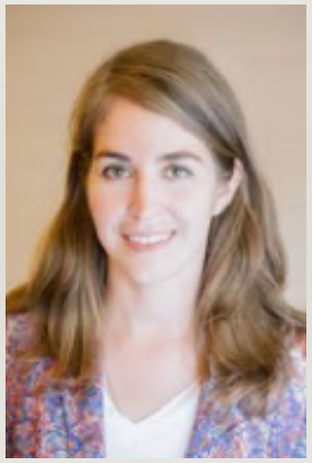
Prism: Scaling Blockchains

Sreeram Kannan
University of Washington Seattle

Vivek Bagaria
Stanford

David Tse
Stanford



Giulia Fanti
CMU

Pramod Viswanath
UIUC

"Sapiens rule the world, because we are the only animal that can cooperate flexibly in large numbers."

- Harari, *Sapiens*

Cooperation requires trust.

Evolution of Trust

PHASE 1

TRIBAL TRUST

PHASE 2

INSTITUTIONAL TRUST

PHASE 3

DISTRIBUTED TRUST

- large-scale
- decentralized
- permission-less

A breakthrough

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

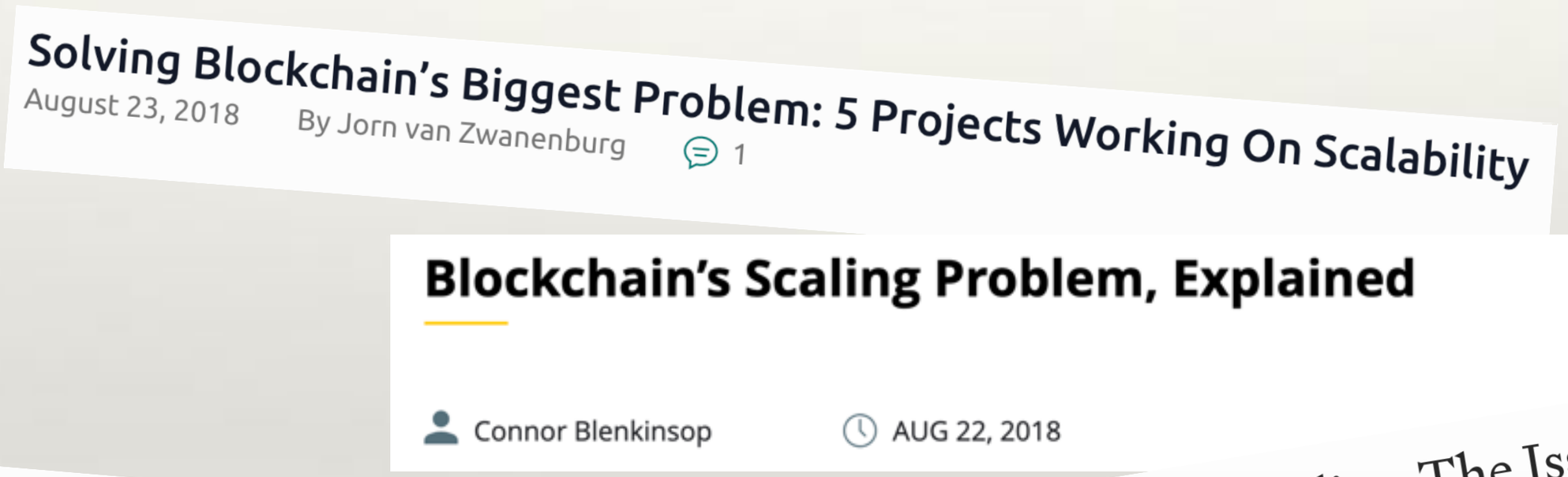
Blockchain

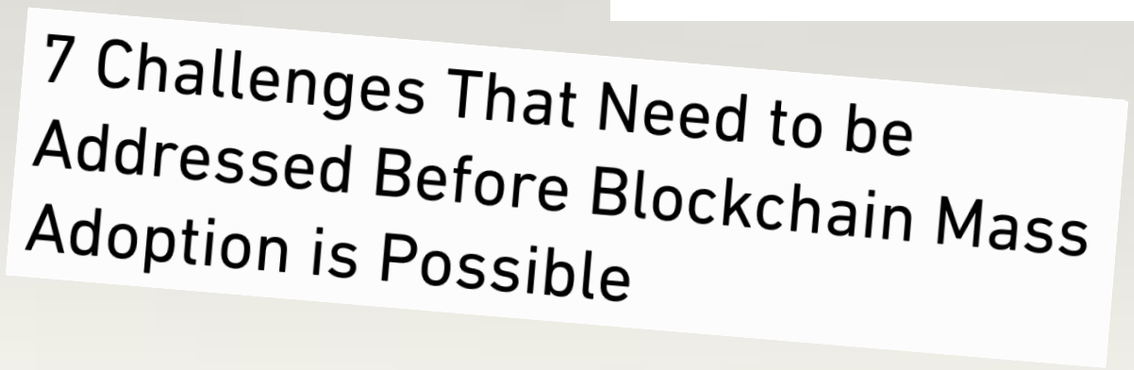
Proof-of-work

Bitcoin performance

	Security	Throughput	Confirmation Latency
Bitcoin	✓	✗	✗
	50% adversary	5 transactions/s	hours

Principal challenge: Scalability

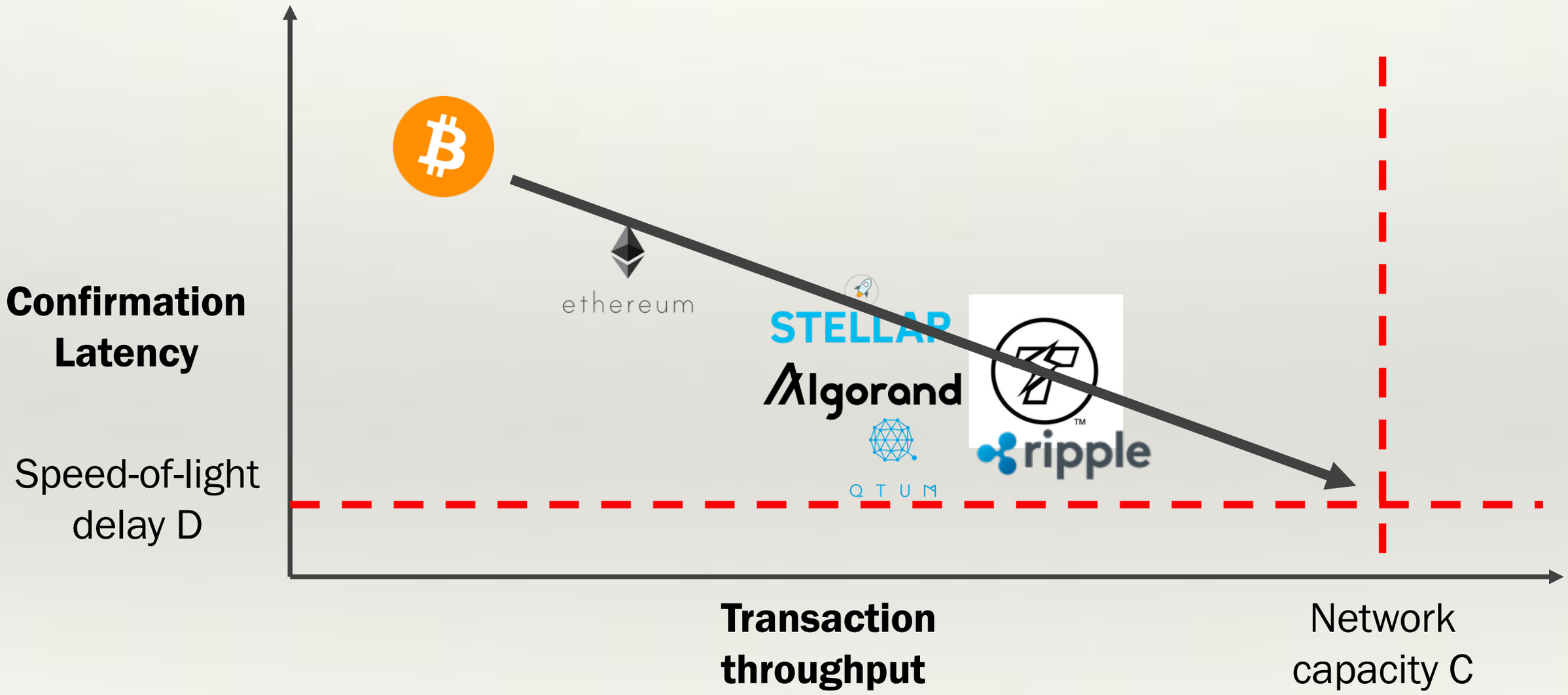




Consensus protocol mania

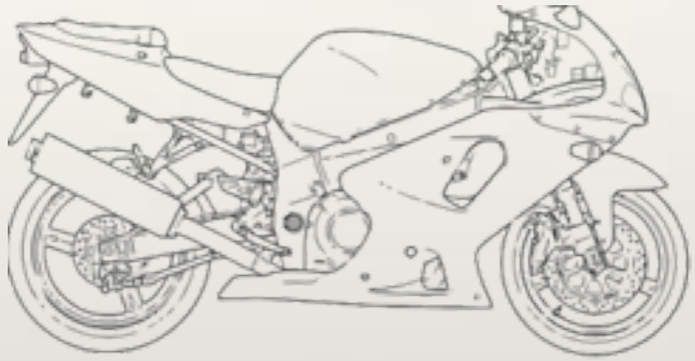
- Different security guarantees and decentralization
- How far can we go?

Physical limits with Bitcoin security?



This work:

Deconstruct
Bitcoin

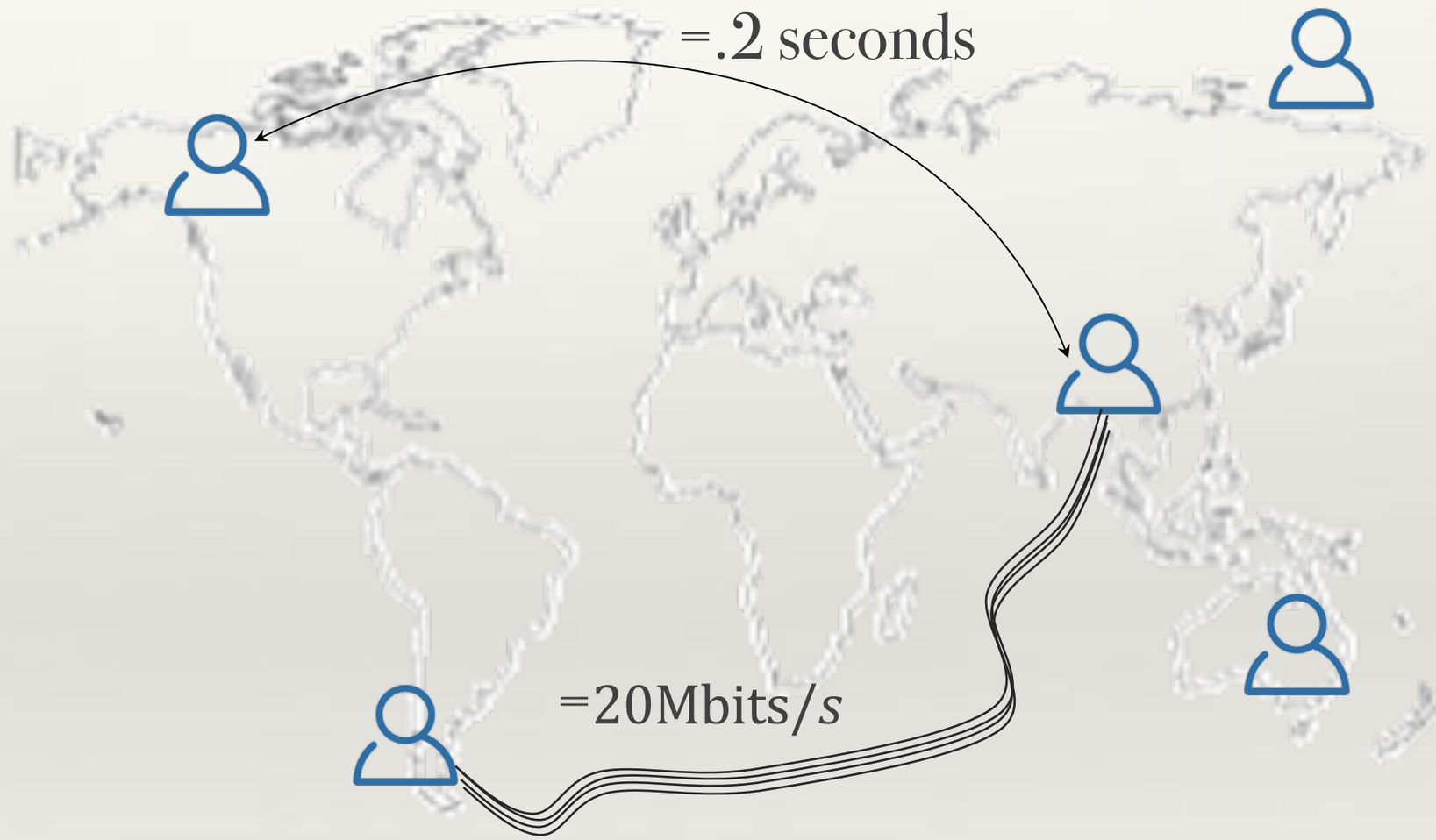


Prism:
Near Physical Limits

Physical Limits

Network capacity C

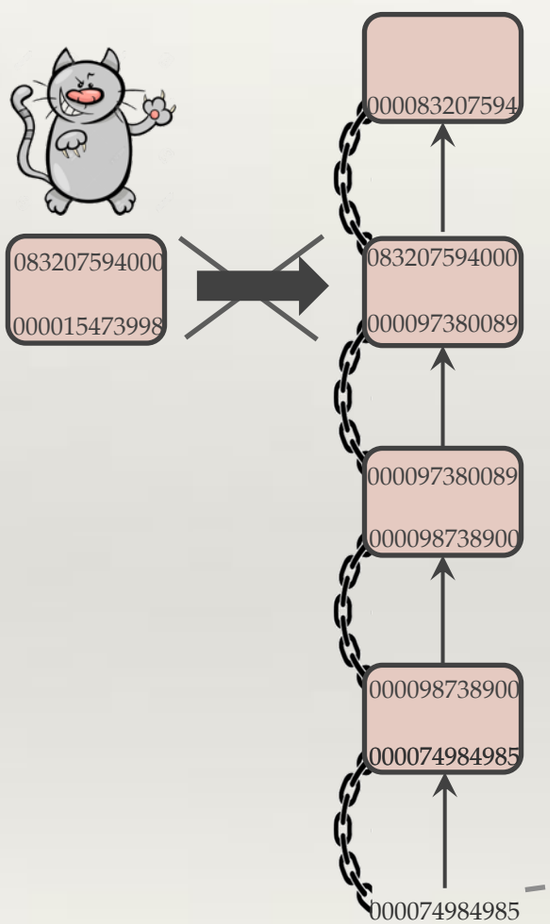
Speed-of-light propagation delay D



Operating near physical limits

	Security	Throughput	Confirmation Latency
Bitcoin	✓ 50% adversary	✗ 5 transactions/s	✗ hours
Prism	✓ 50% adversary	✓ ~ C	✓ ~ D

Ledger


Blockchain
000083207594
083207594000
000015473998
083207594000
000097380089
000097380089
000098738900
000098738900
000074984985
000074984985
000019234344
Hash of previous block *Prev*
Proof-of-work
Transactions *Tx*
000074984985
000019234344
Hash(*Prev*, *Tx*, *nonce*) < threshold
?
Mining new block

BTC.com Pool Wallet Blocks Stats Tools Applications BCH Ethereum (ETH) NEW Address/Height/Hash...

Latest Blocks

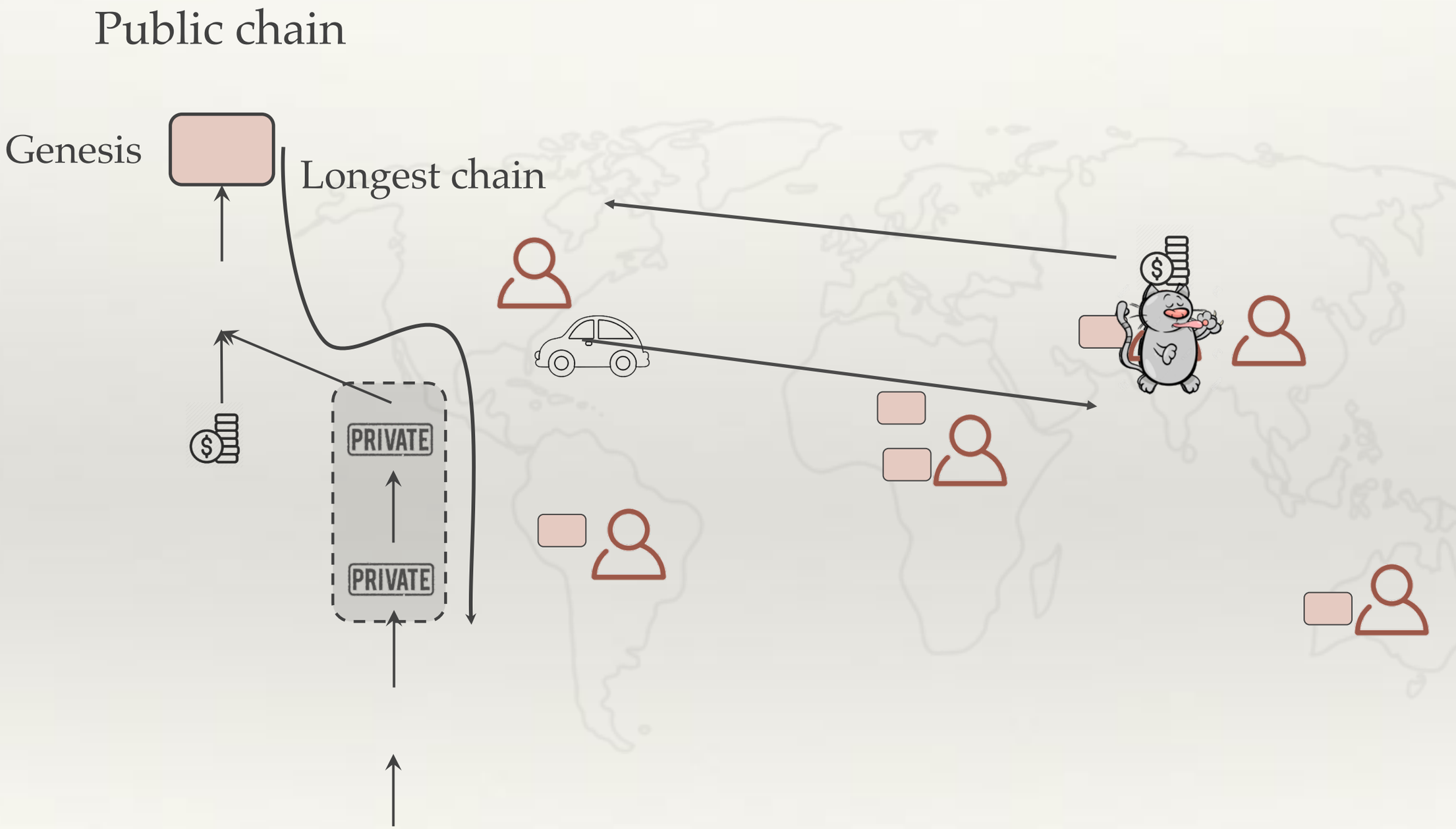
Height	Relayed By	Size(B)	Reward	Time	Block Hash
549,509	WAYI.CN	1,016,939	13.20501009 BTC	39 minutes ago	0000000000000000000233385 2dbc8af5c643cd866d4baf40da52f2d60dc66997
549,508	BTC.com	1,355,438	12.74596921 BTC	1 hour 34 minutes ago	000000000000000000018b1dd864104e16acecc4ce48e4eb13df110f2d625fb25
549,507	SlushPool	1,173,457	12.92437274 BTC	1 hour 54 minutes ago	0000000000000000000e79ecc242e82e17b4625011553d9bc5097fefd3bb2003
549,506	ViaBTC	1,209,185	12.63095738 BTC	3 hours 19 minutes ago	000000000000000000023af7b0b43ae1a34098a7979f4ca56350866f114822acc
549,505	BitFury	91,668	12.51600930 BTC	3 hours 32 minutes ago	000000000000000000f382fadaf28f14815ed5ccaf9a54c1cf0c17be269f49e
549,504	F2Pool	189,065	12.51737065 BTC	3 hours 34 minutes ago	000000000000000000e94ae4d32c85fcc90a65a7dda90260de9c24d467e9c89
549,503	Bixin	530,828	12.55331001 BTC	3 hours 37 minutes ago	000000000000000000021eb420f7e8444c47c97151661 7c423d8c9962bdecb14a
549,502	unknown	506,409	12.51435953 BTC	3 hours 42 minutes ago	000000000000000000027d9e092926f385f4949fa3a9a300dec4577766a6ef68
549,501	BitFury	278,177	12.55413130 BTC	3 hours 42 minutes ago	000000000000000000230e352c577f8b6245691ea660e8972d8df284e5910bf8
549,500	BTC.com	12,640	12.50167957 BTC	3 hours 48 minutes ago	000000000000000000b17f8520cb68cbe11f3e341e23d30dd7dbb738cdde779

Distributed ledger

Public chain

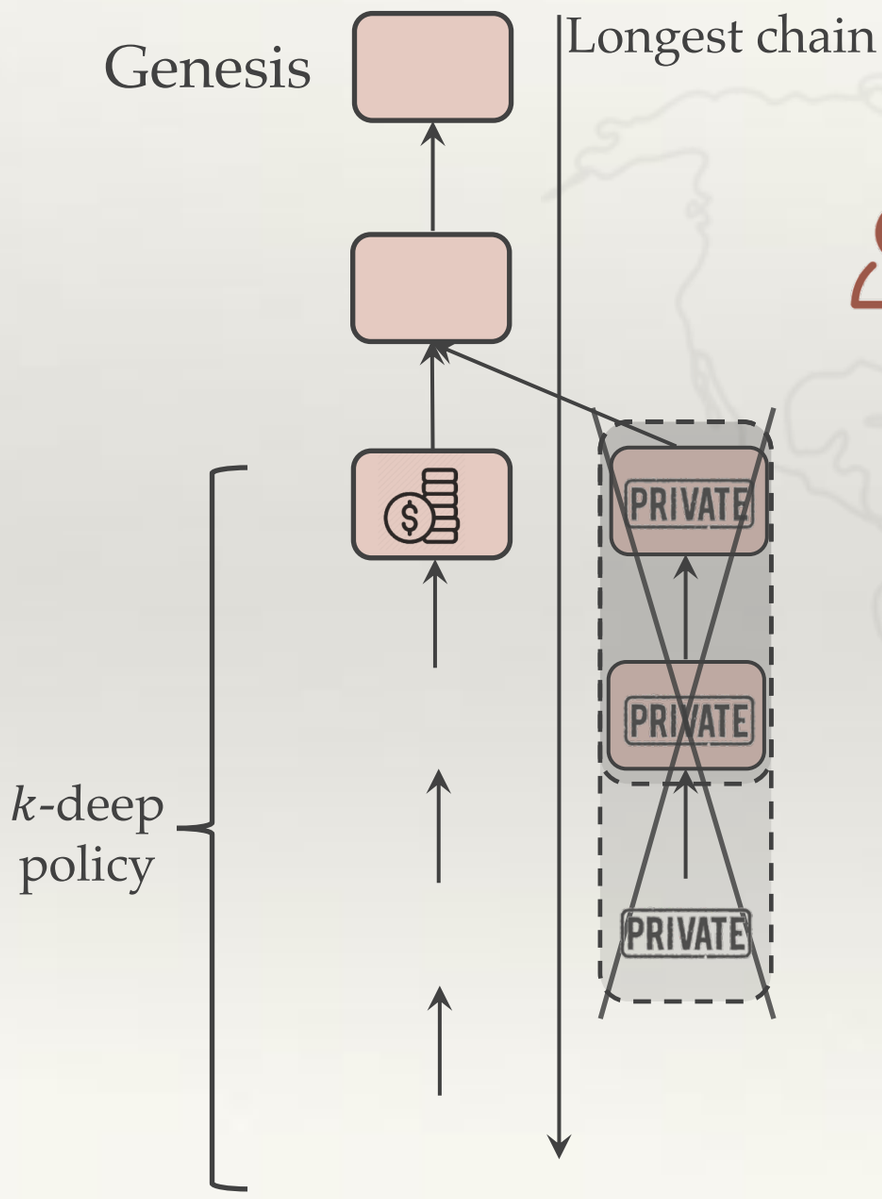
- Poisson process
- longest chain protocol

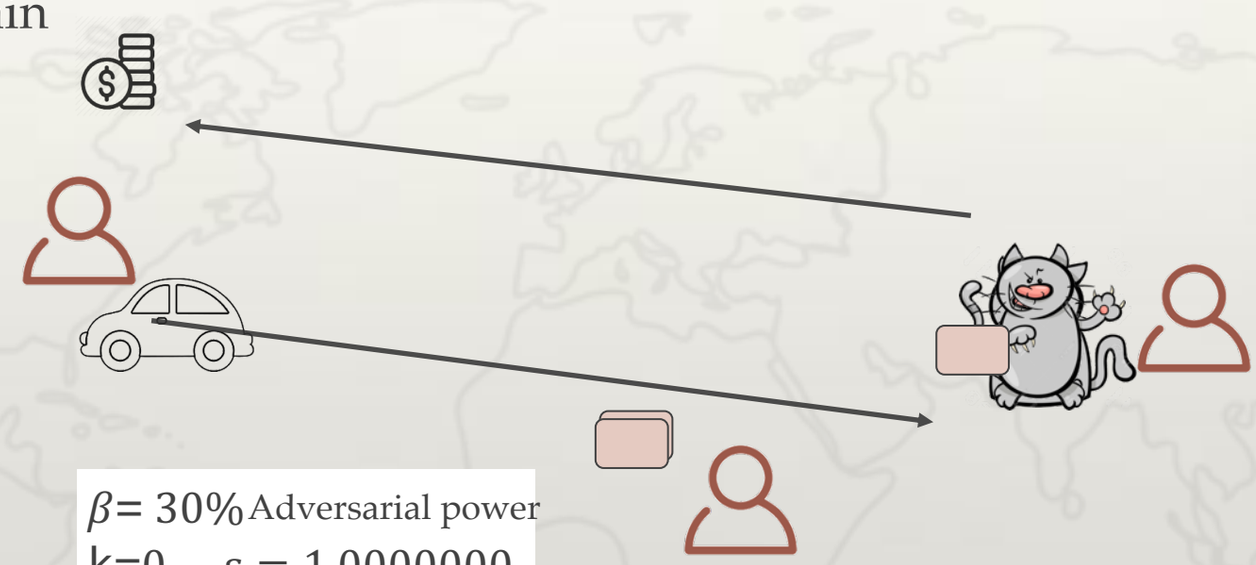
Private double-spend attack



Defense: k-deep confirmation

Public chain





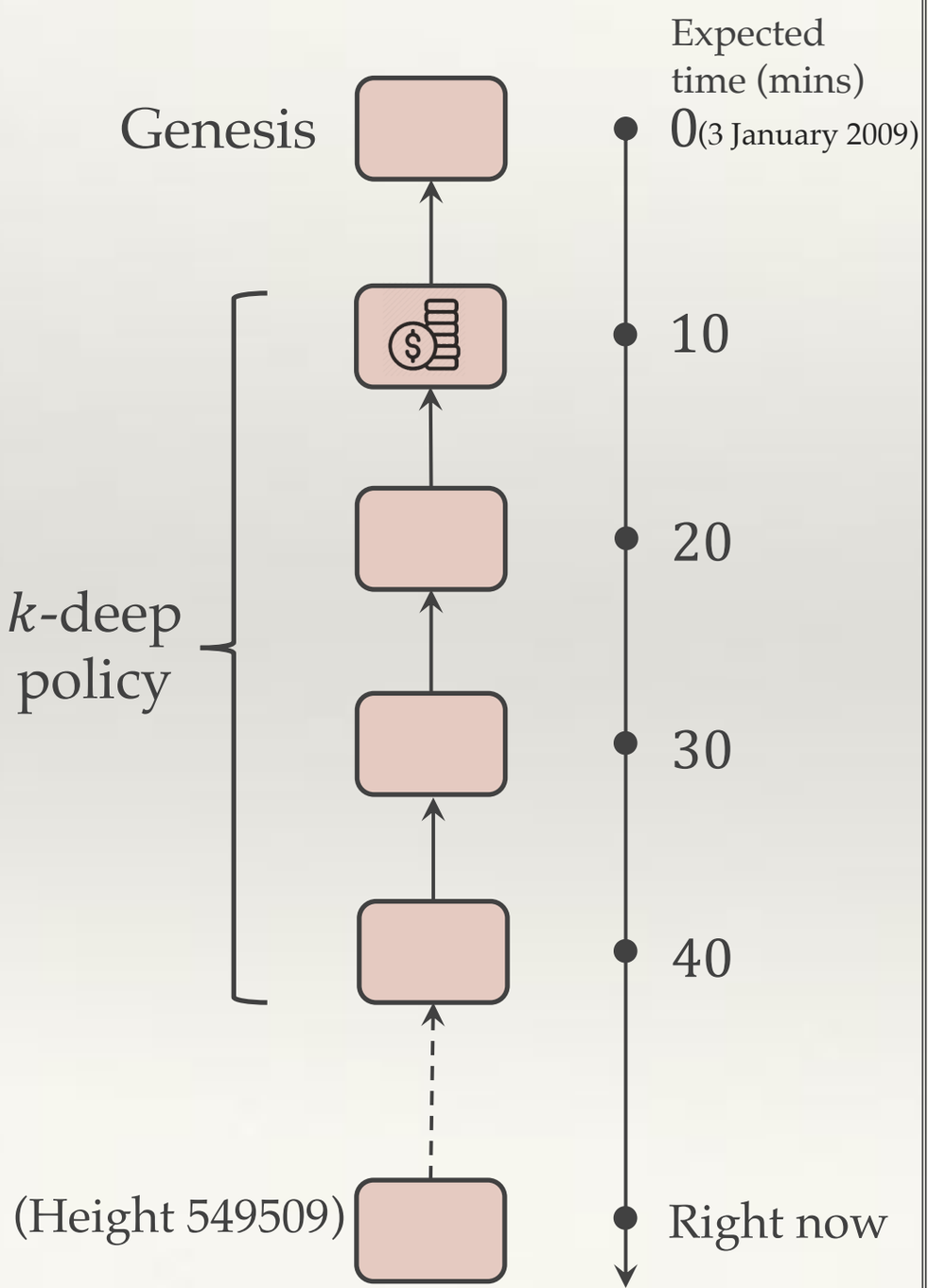
β= 30%	Adversarial power
k=0	$\varepsilon = 1.0000000$
k=5	$\varepsilon = 0.1773523$
k=10	$\varepsilon = 0.0416605$
k=15	$\varepsilon = 0.0101008$
k=20	$\varepsilon = 0.0024804$
k=25	$\varepsilon = 0.0006132$
k=30	$\varepsilon = 0.0001522$
k=35	$\varepsilon = 0.0000379$
k=40	$\varepsilon = 0.0000095$
k=45	$\varepsilon = 0.0000024$
k=50	$\varepsilon = 0.0000006$

Nakamoto's table

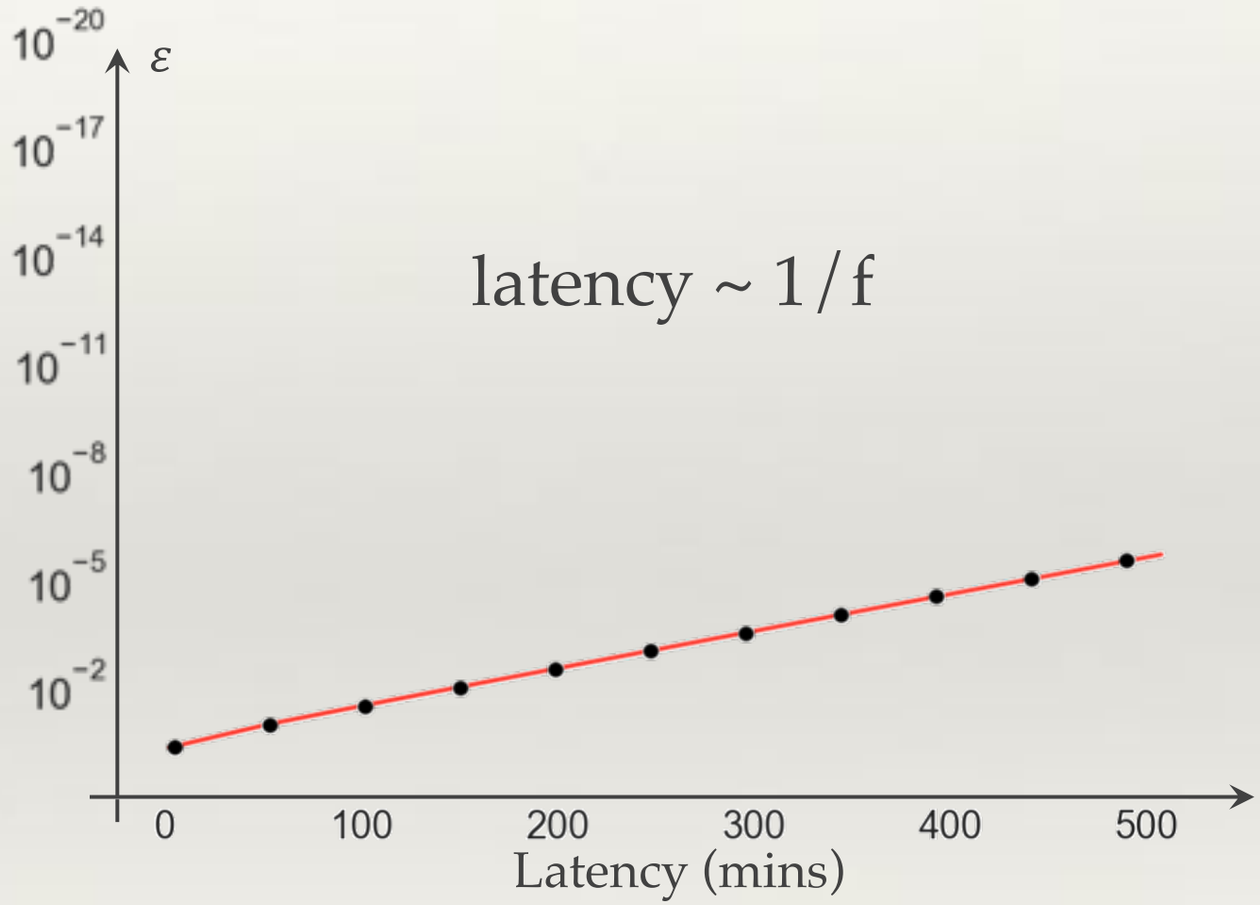
- Law of large numbers!
- Tolerate attack up to 50% adversarial power

Latency and throughput

Public chain



Mining rate: $f = 1$ block/10 min



latency ~ 1/f

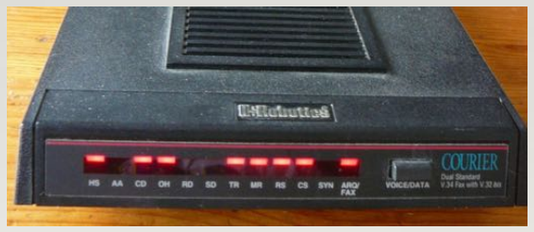
throughput ~ f

Physical limits

Bitcoin mining rate f = 1 block/ 10 min

Bitcoin bandwidth consumption ~ 20 kbits/seconds

1994

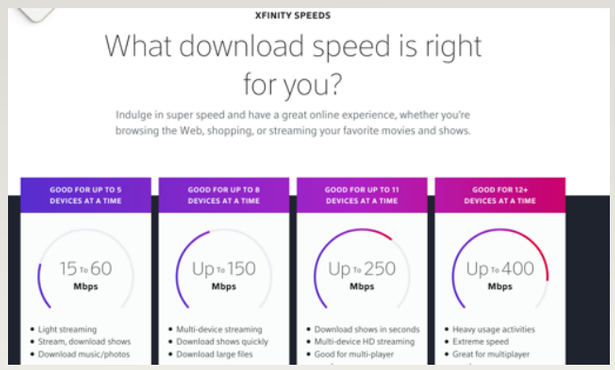


V.34 modem

C = 28.8 kbps

1000 to 10,000 X

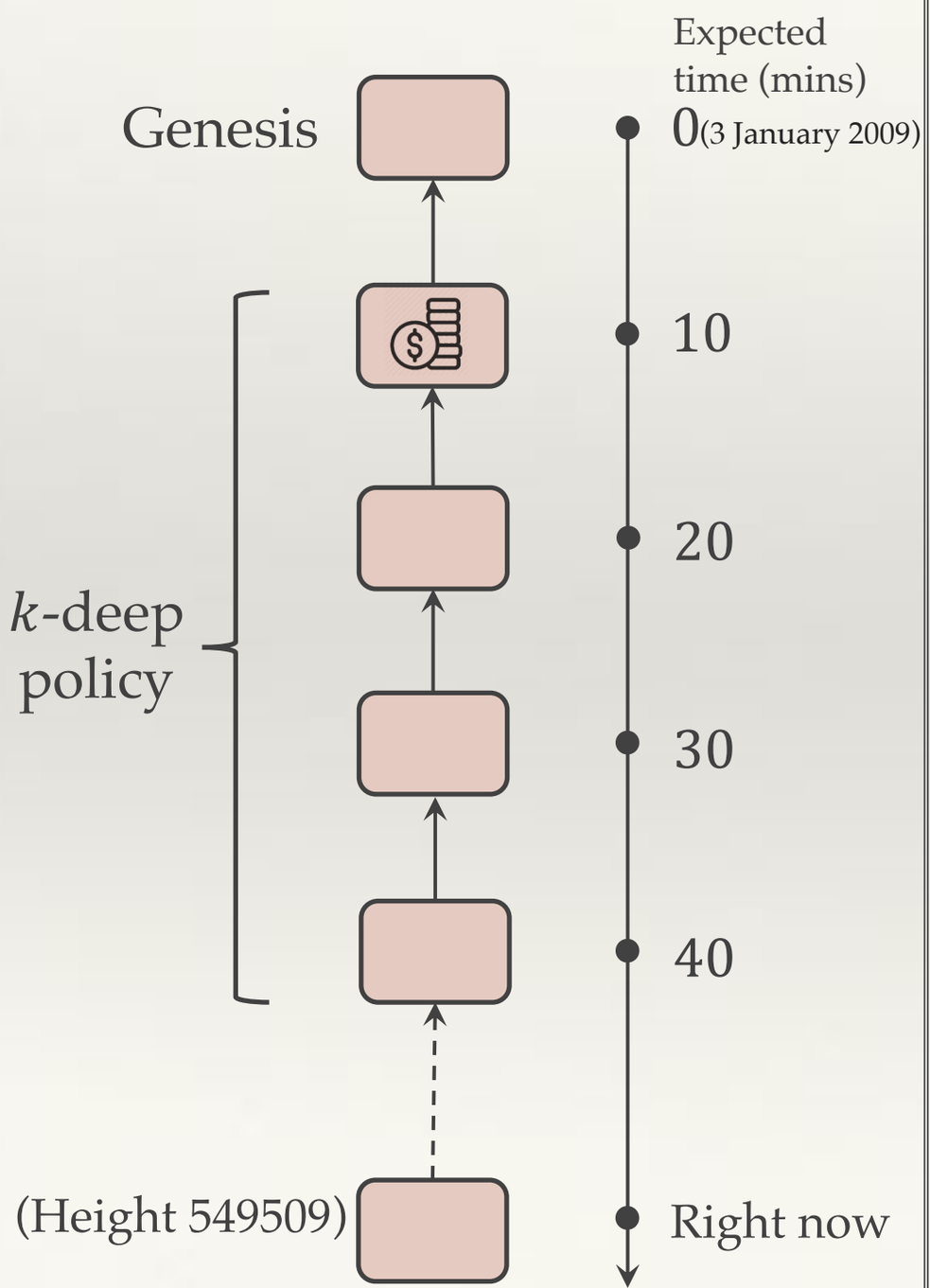
2018



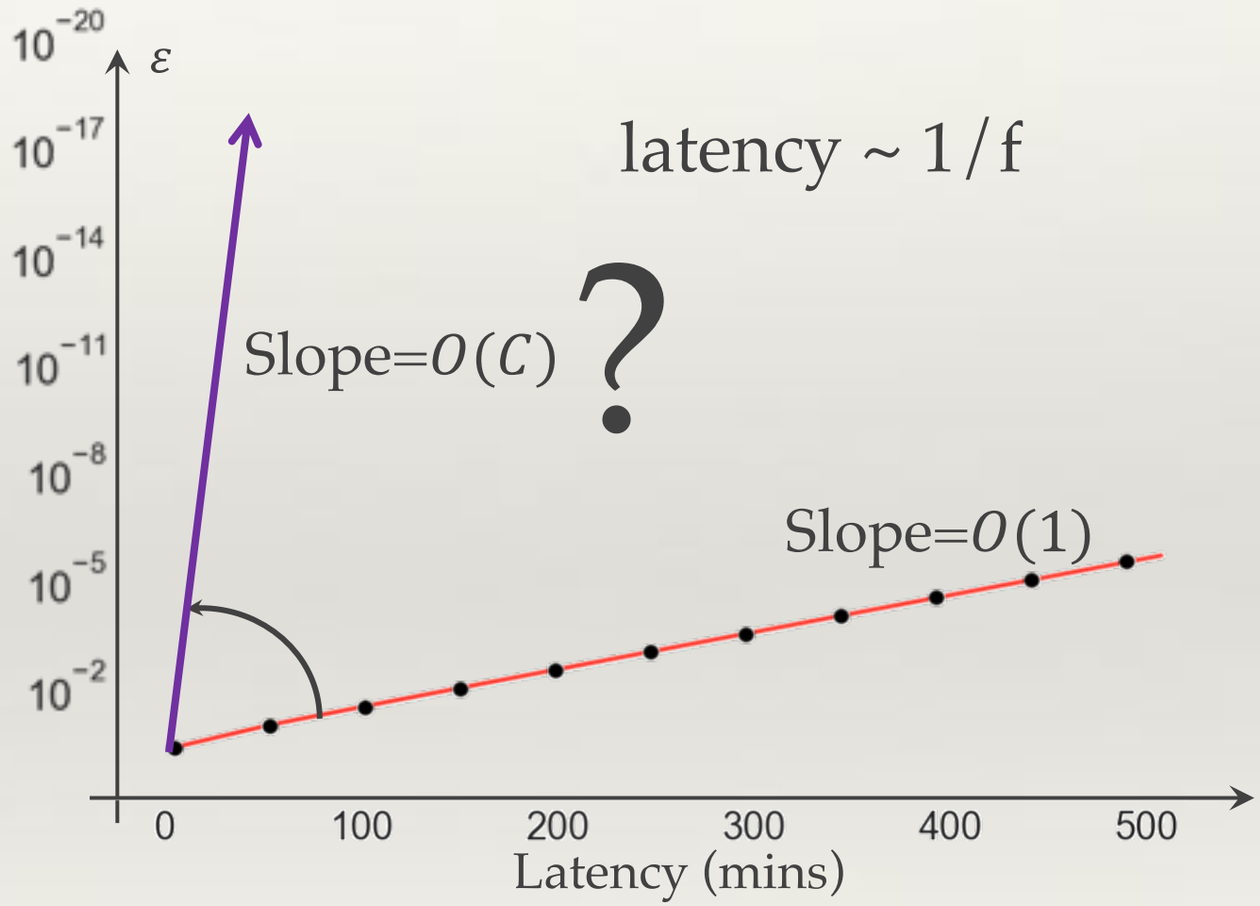
C = 10-100's Mbps

Latency and throughput

Public chain



Mining rate: $f = 1$ block/10 min



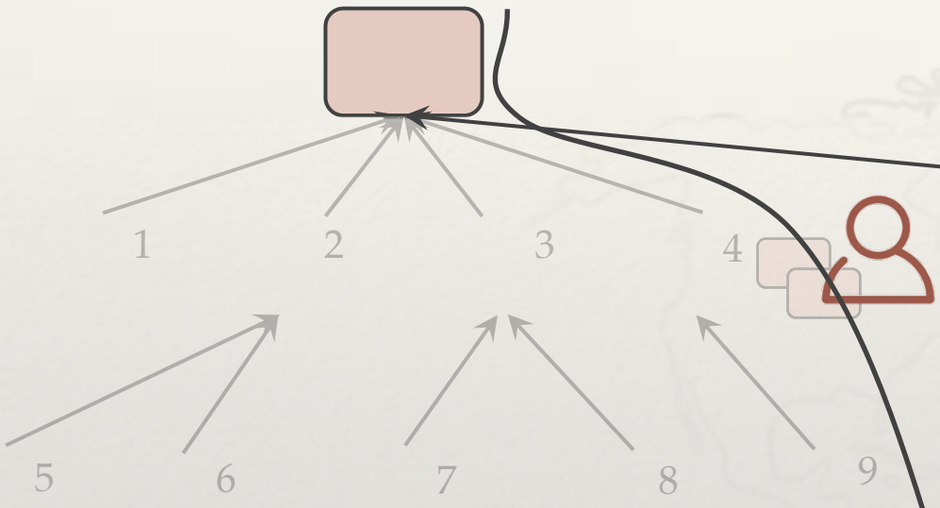
Increase mining rate f

Cryptographic puzzle:

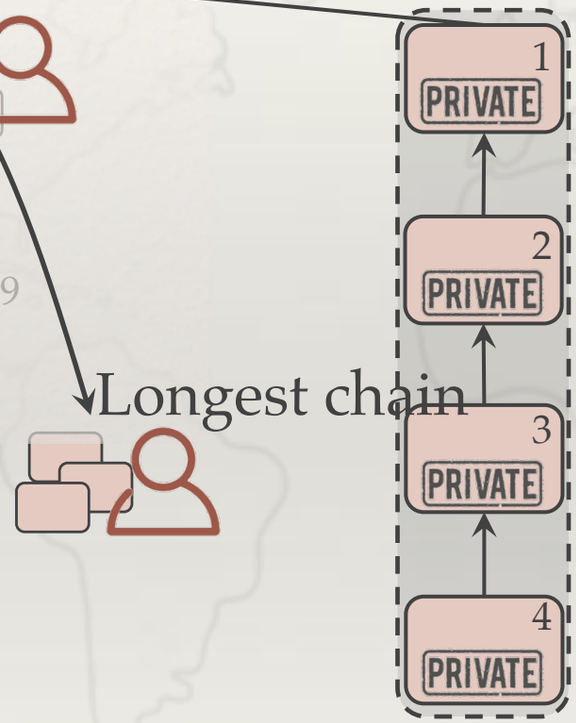
$$\text{Hash}(Prev, Tx, \boldsymbol{nonce}) < \text{threshold}$$

increase threshold → easier puzzle → increase f

Forking

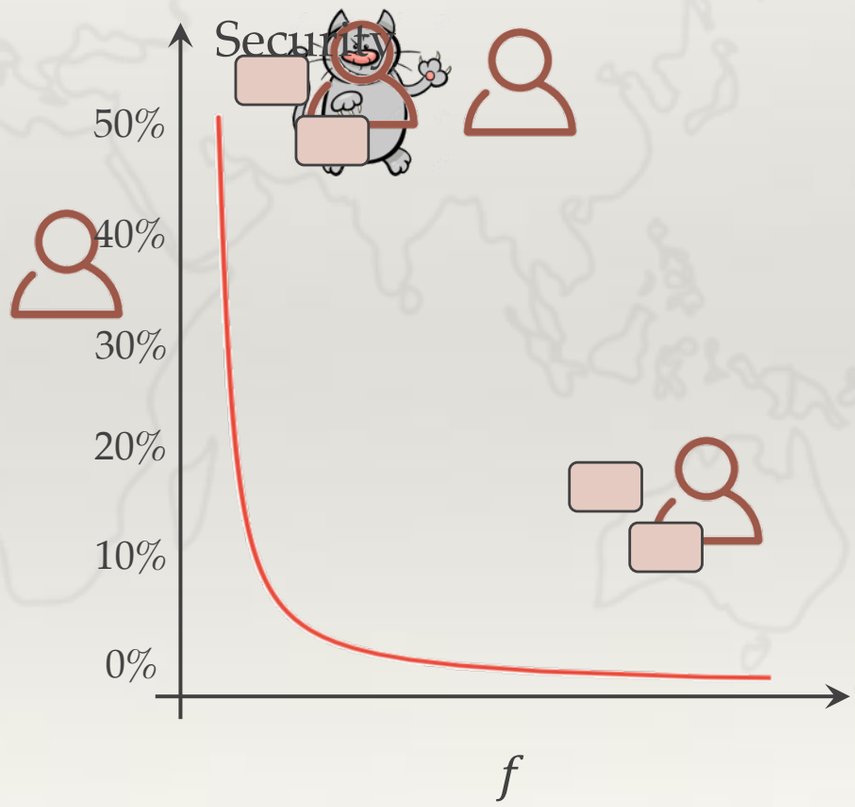


Network delay Δ
leads to forking and
slows growth



Change protocol?

GHOST, Inclusive, Spectre, Phantom, Conflux ……



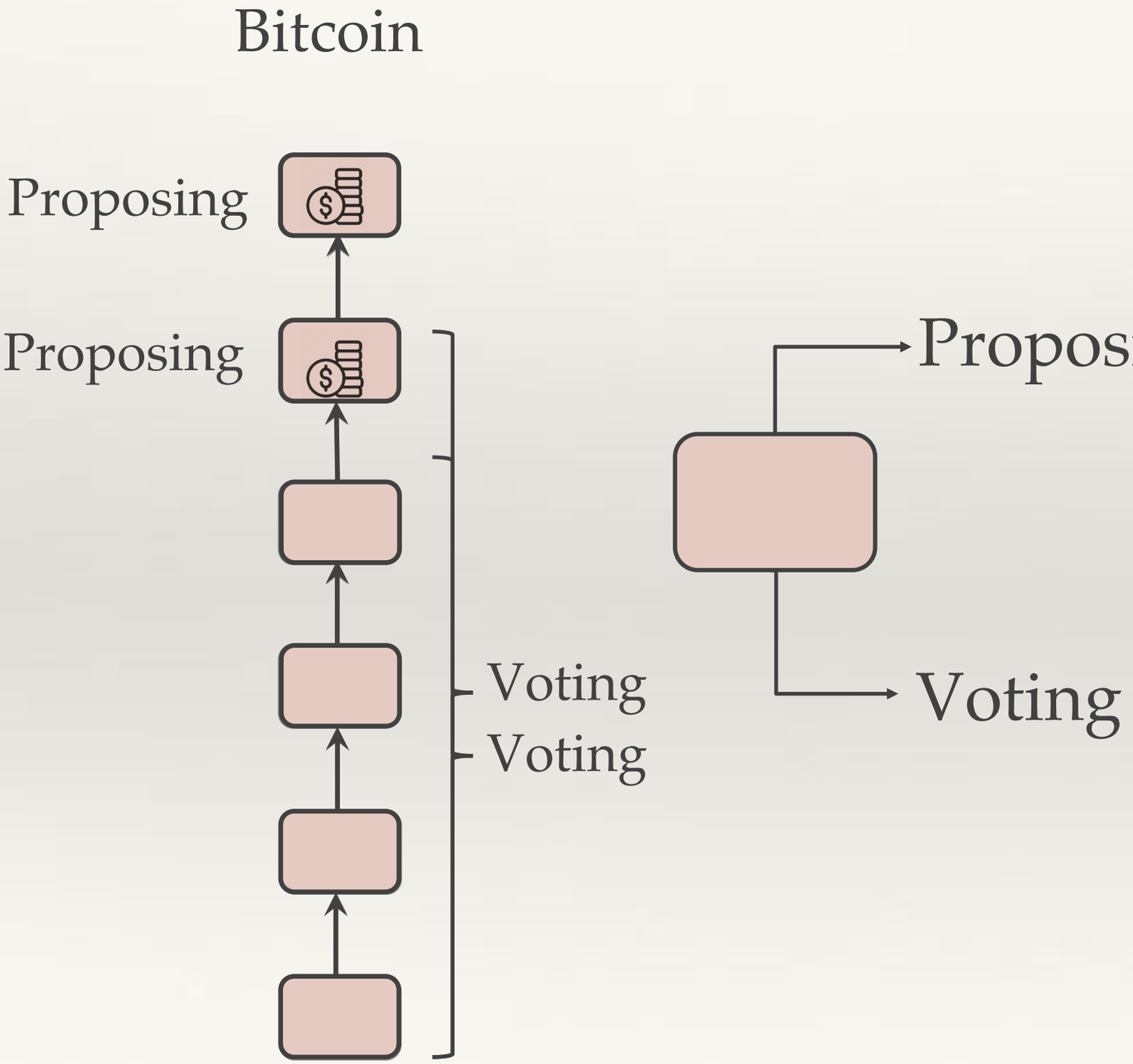
Natoli & Gramoli. The balance attack against proof-of-work blockchains: The r3 testbed as an example, 2016

1. Hard to beat longest chain design.

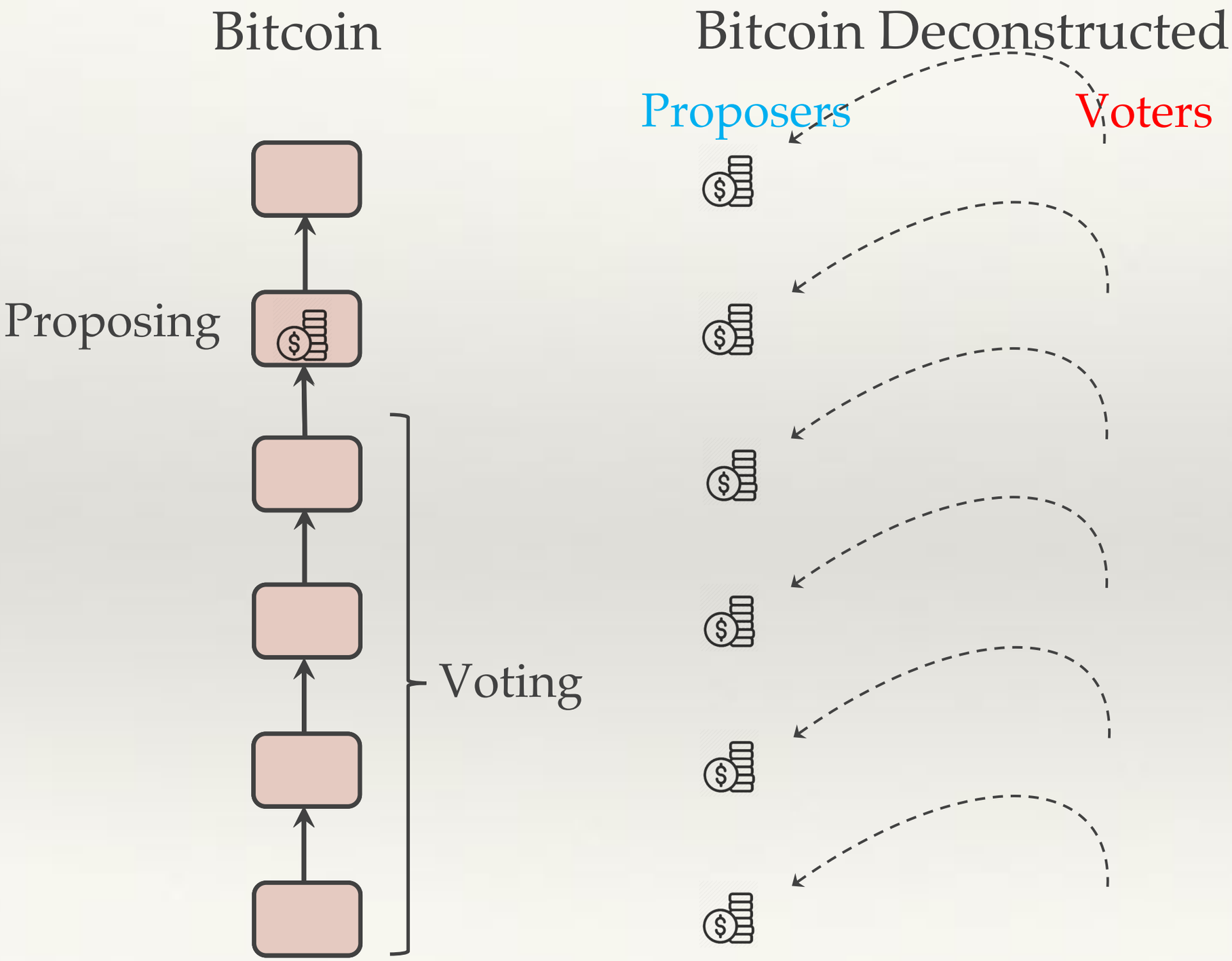
2. Formal security analysis required.

"Bitcoin Backbone protocol" Garray et al, 2016

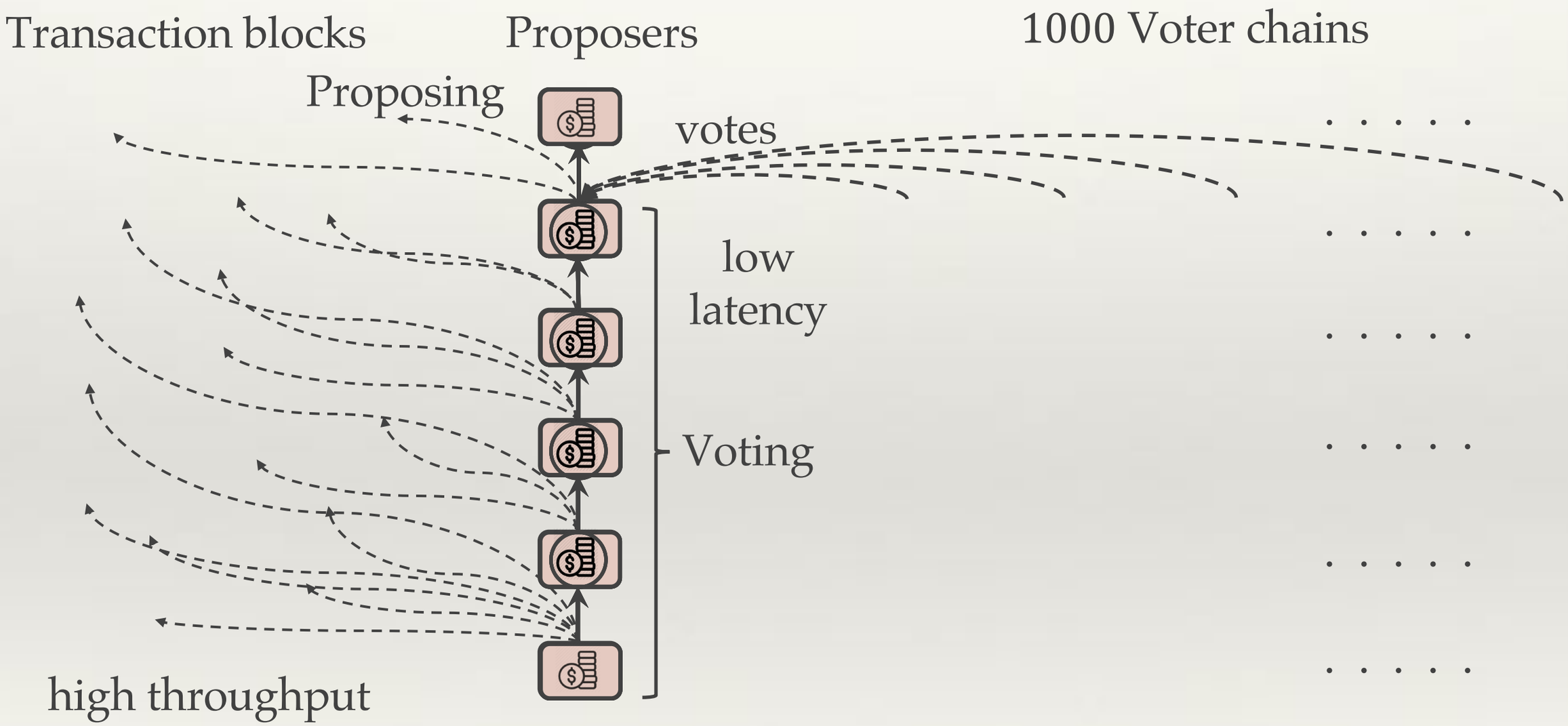
2 roles of a block



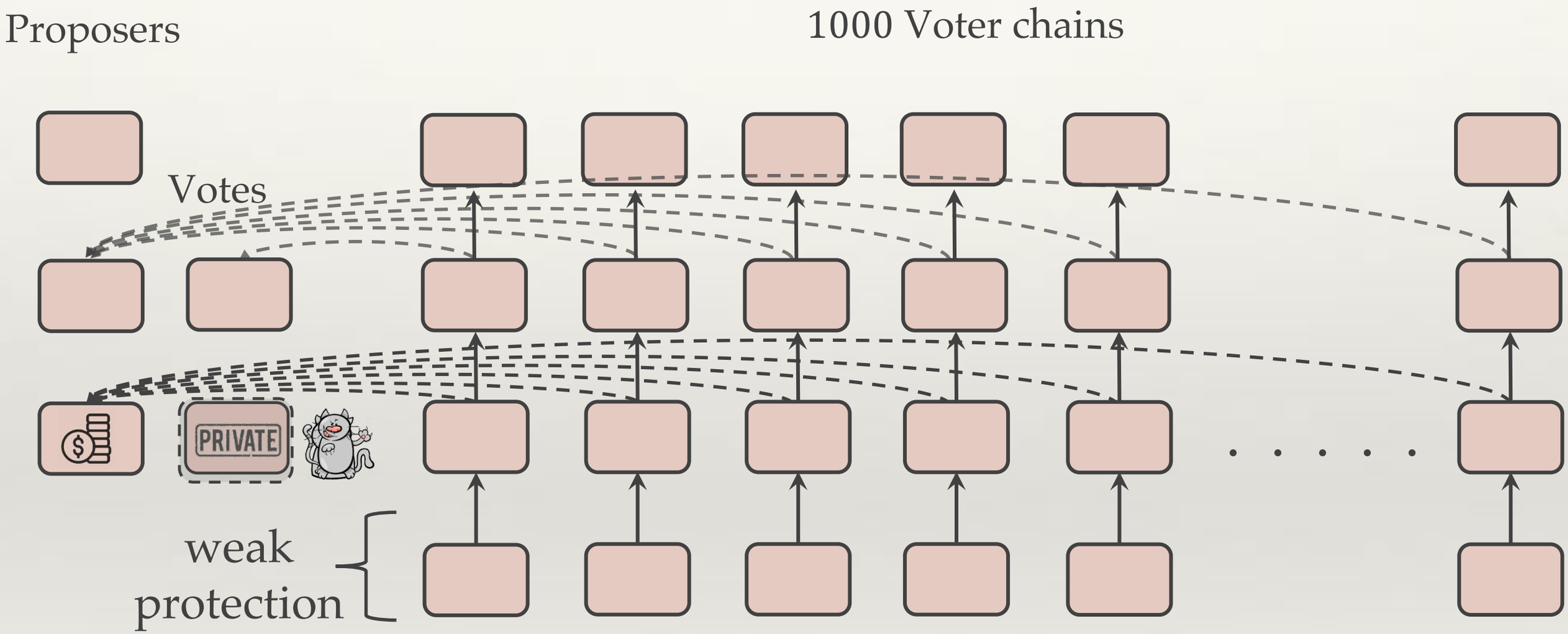
Deconstruction



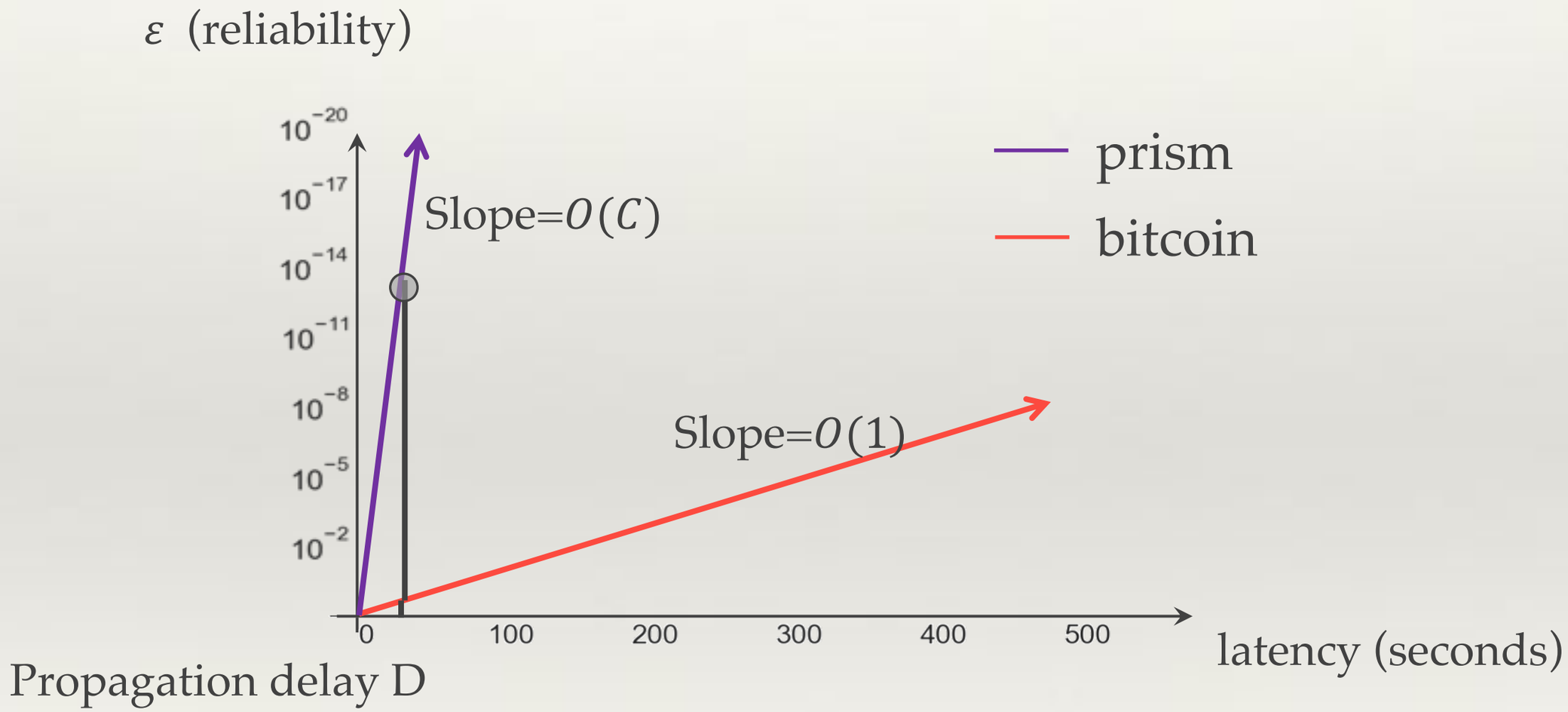
Prism


Transaction blocks
Proposers
1000 Voter chains
Proposing
votes
low
latency
Voting
high throughput

Law of large numbers



Prism: latency



$$\log \frac{1}{\epsilon} \propto C \cdot D$$ bandwidth-delay product

Prism: formal guarantees

Theorem:

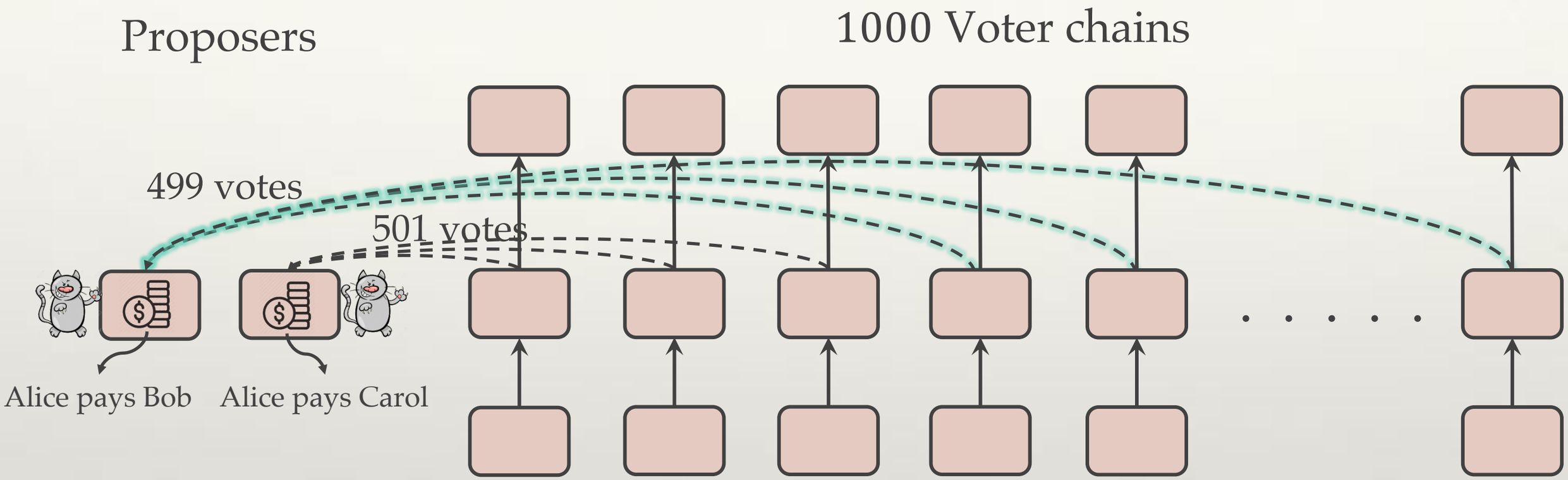
As long as the adversarial power β is less than 50%, Prism is guaranteed to :

1) confirm honest transactions with delay proportional to D and reliability exponentially small in the bandwidth-delay product CD.

2) create a totally ordered ledger of all transactions with persistency and liveness properties.

3) achieves optimal throughput of $(1-\beta)C$

Public double-spends

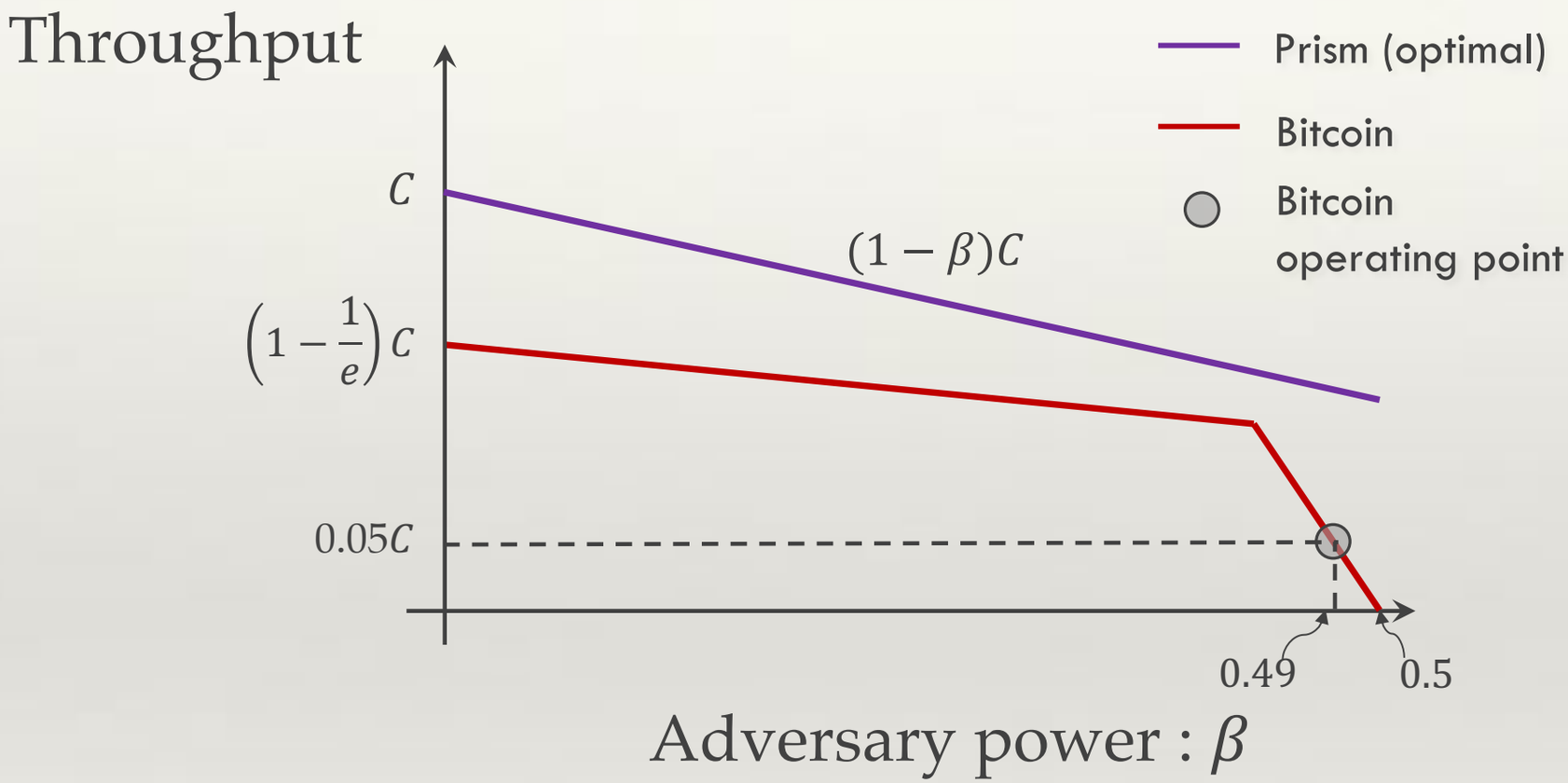


Can we now confirm the block with 501 votes? No.

But can now confirm that one of the two blocks is in the final ledger.

Eventually will be able to confirm which one.

Prism: optimal throughput



Prism: Sortition

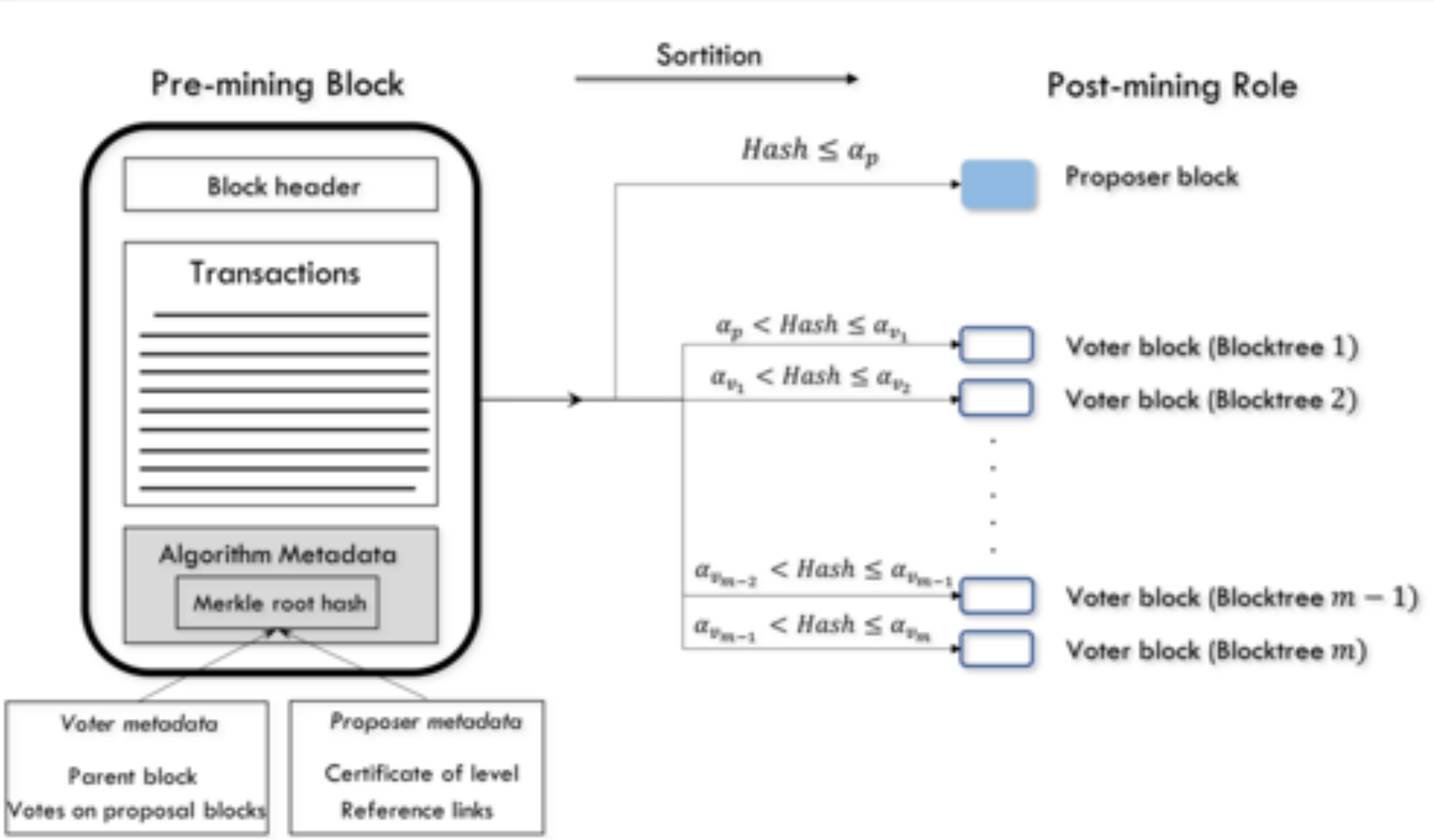
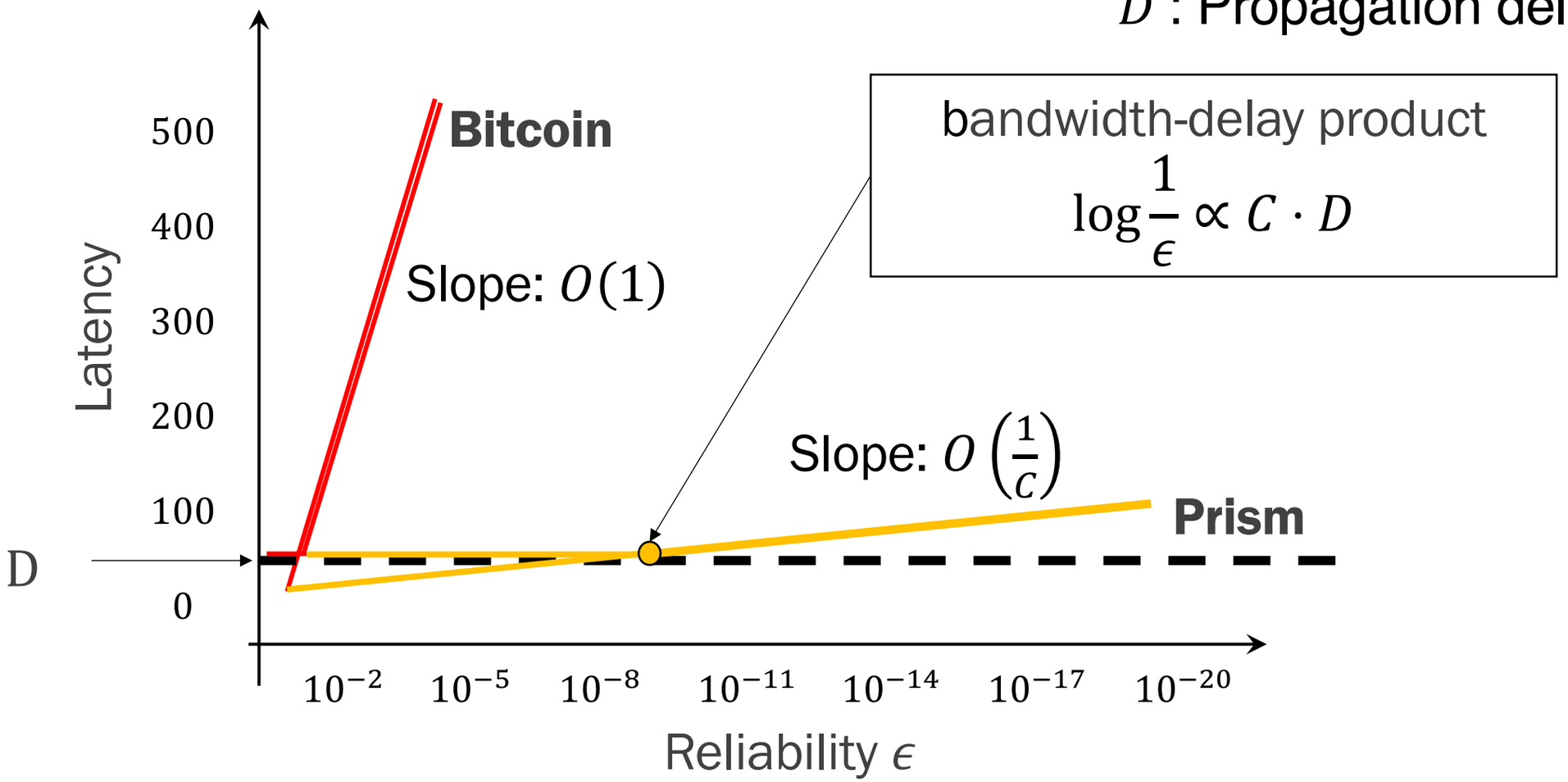


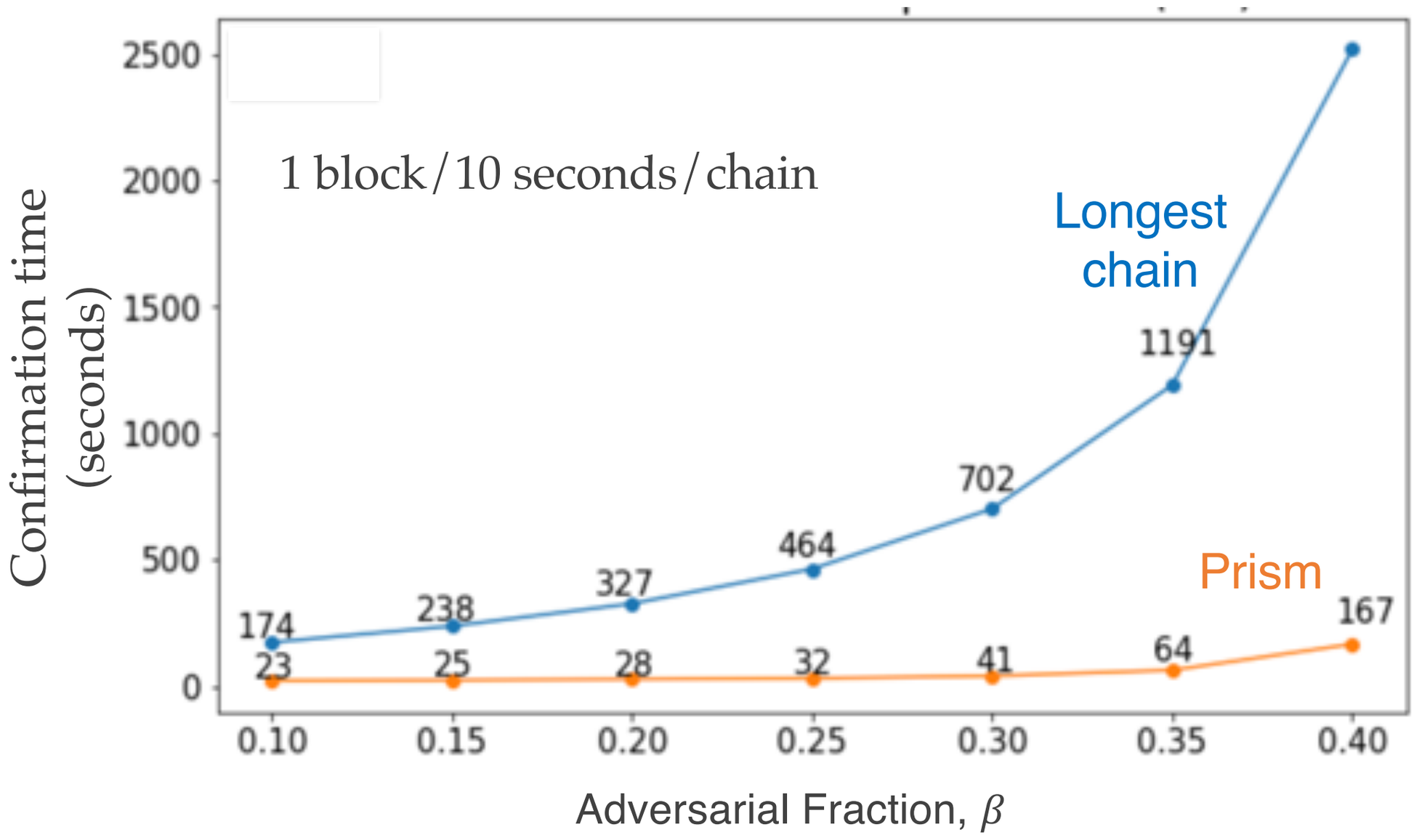
Fig. 11: Summary of the block structure and the sortition procedure.

Latency scaling

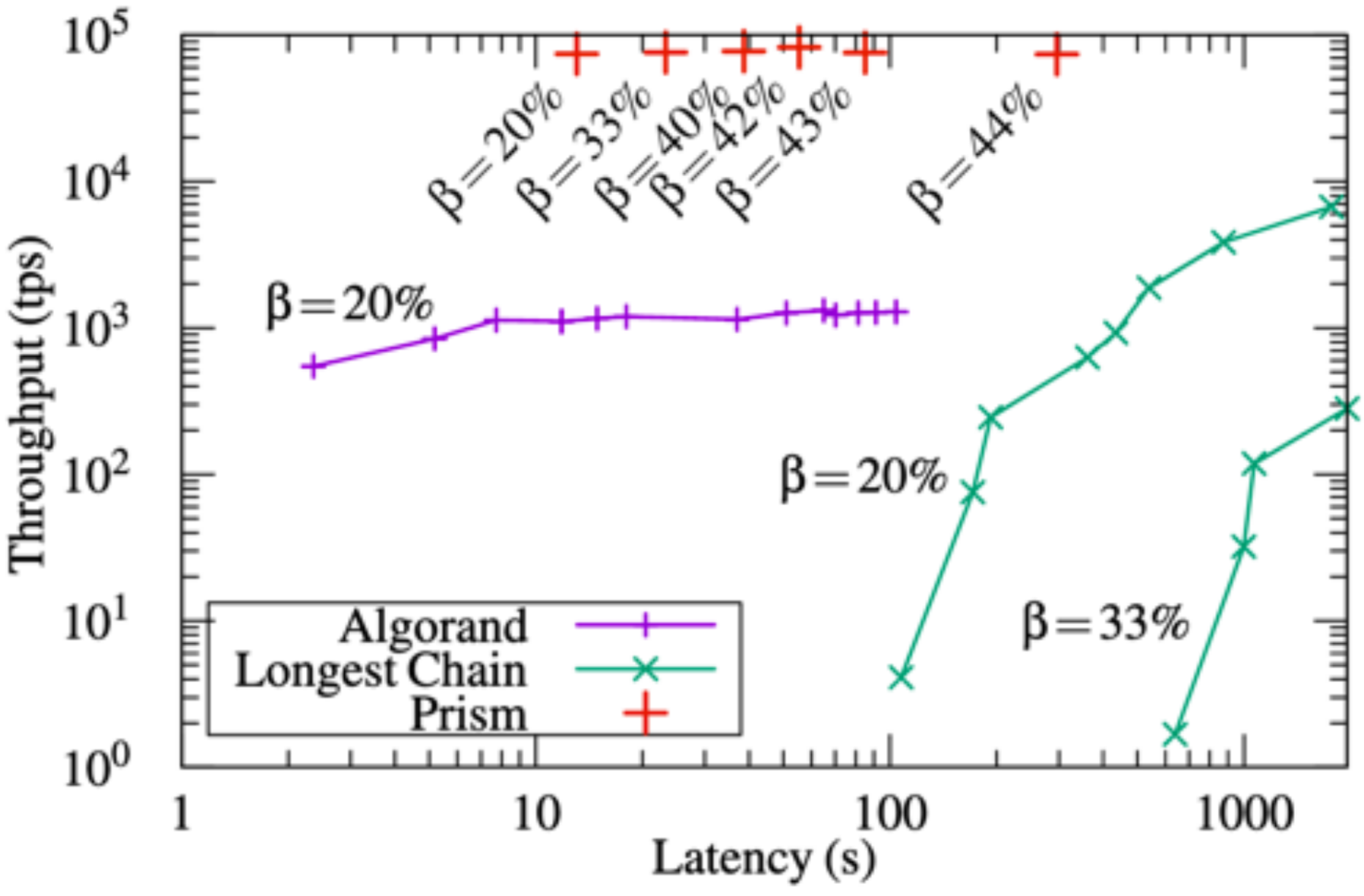
C : Network capacity
D : Propagation delay



Simulated Latency



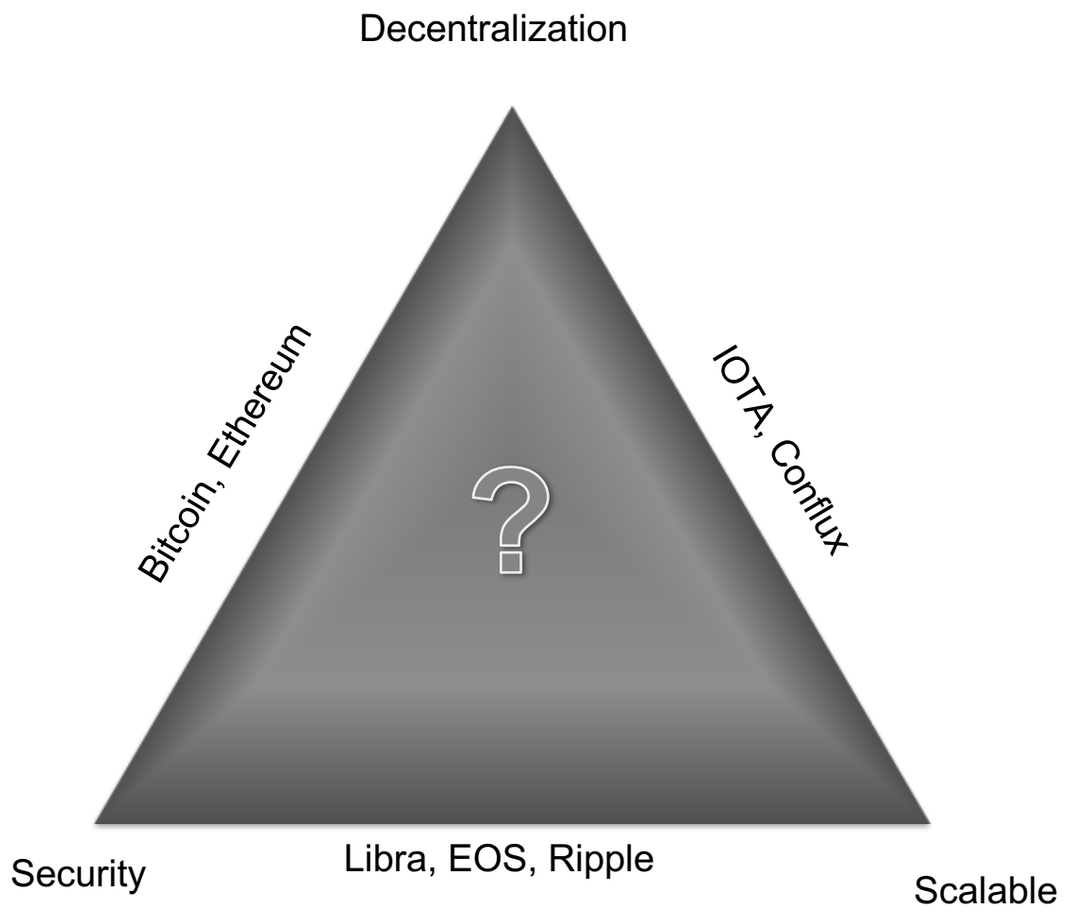
Real Implementation in Rust



Lei Yang, .., Mohammad Alizadeh, “Prism: Scaling bitcoin by 10,000x”

The blockchain trilemma

Existing blockchains can only provide two out of three features: **Blockchain Trilemma**



The blockchain trilemma